UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/827,082	04/19/2004	Christopher G. Kaler	13768.506	1874

22913 7590 05/04/2007
WORKMAN NYDEGGER
(F/K/A WORKMAN NYDEGGER & SEELEY)
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
ZEE, EDWARD	
ART UNIT	**PAPER NUMBER**
2109	

MAIL DATE	DELIVERY MODE
05/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/827,082	KALER ET AL.	
	Examiner	Art Unit	
	Edward Zee	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the original filing date of April 19, 2004. Claims 1-33 are pending and have been considered below.

Claim Objections

2. Claim 1 is objected to because of the following informalities: the examiner notes a typographical error "that that" on line 14 of this claim. Appropriate correction is required.

3. Claims 2 and 9 are objected to because of the following informalities: the examiner notes the use of the acronym "SSL" in these claims without first including a description in plain text, as required. Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 31-33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 31-33 are drawn to computer readable media, which the applicant has defined in the specification [page 11, paragraph 0029] to encompass an electronic transmission signal. The Office considers an electronic signal to be a form of energy. Energy is not a series of steps or acts and this is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a compilation of matter. Thus, an electronic transmission signal does not fall within any of the four categories of invention. Therefore, claims 31-33 are not statutory.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 3-5, 8, 10, 11, 21-30, 32 and 33 are rejected under 35 U.S.C. 102(b) as being anticipated by Traw et al. (6,542,610).

Claim 1: Traw et al. discloses a method for providing information that can be used to verify measurable aspects of a requesting computing system, the method comprising:

a. an act of performing at least one of determining that the providing computing system*(Device A)* is appropriately configured to issue challenges to components included in the requesting computing system*(Device B)* and determining that the providing application is appropriately configured to issue challenges to the requesting instructions*(Device A sends a challenge to Device B and compares the response to an expected value)* [column 7, lines 16-41];

b. an act of subsequently accepting a challenge that was initiated by the providing application based at least in part on the providing computing system and the providing application being appropriately configured to issue challenges to the requesting instructions*(following successful completion of the preliminary authentication procedure, each device calculates and exchanges signed messages)* [column 8, lines 33-39];

c. and an act of submitting an assertion that can be used to verify that the requesting instructions are configured in accordance with one or more measurable aspects that are

appropriate for interacting with the providing application*(signed messages)* [column 8, lines 33-39].

Claim 3: Traw et al. discloses a method as in claim 1 above and further discloses that the act of determining that the providing application is appropriately configured to issue challenges to the requesting instructions comprises receiving proof that the providing application complies with one or more security and trust policies of the requesting computing system*(compares data string to expected value to determine if devices can exchange protect content)* [column 7, lines 16-41].

Claim 4: Traw et al. discloses a method as in claim 1 above and further discloses that the act of subsequently accepting a challenge that was initiated by the providing application comprises an act of subsequently accepting a request for proof of the values*(signed message)* of one or more measurable aspects of the requesting computer system*(Device B transmits signed message to Device A)* [column 8, lines 33-39]. The examiner notes that the act of transmitting a proof value to Device A implies that Device B has accepted a request for a proof value.

Claim 5: Traw et al. discloses a method as in claim 1 above and further discloses that the submitted assertion includes the values of one or more measurable aspects of the requesting computer system*(signed message contains random challenge and Diffie-Hellman key exchange value)* [column 8, lines 33-39].

Claim 8: Traw et al. discloses a method for verifying measurable aspects of the requesting computing system, the method comprising:

a. an act of performing at least one of proving that the providing computing system*(Device A)* is appropriately configured to issue challenges to components of the requesting computing system*(Device B)* and proving that the providing application is appropriately

configured to issue challenges to the requesting instructions*(each device verifies that the appropriate response has been received)* [column 7, lines 16-41];

b. an act of subsequently causing a configuration challenge to be issued to the requesting instructions*(following successful completion of the preliminary authentication procedure, each device calculates and exchanges signed messages)* [column 8, lines 33-39];

c. an act of receiving an assertion that can be used to verify that the requesting instructions are configured in accordance with one or more measurable aspects that are appropriate for interacting with the providing application*(signed messages)* [column 8, lines 33-39];

d. and an act of validating the assertion*(determines whether message signature is valid)* [column 8, lines 50-56].

Claim 10: Traw et al. discloses a method as in claim 8 above and further discloses that the act of proving that the providing application is appropriately configured to issue challenges to the requesting instructions comprises an act of sending proof*(data string)* that the providing application complies with one or more security and trust policies of the requesting computing system*(compares data string to expected value to determine if devices can exchange protect content)* [column 7, lines 16-41].

Claim 11: Traw et al. discloses a method as in claim 8 above and further discloses that the act of subsequently causing a challenge to be issued to the requesting computing system comprises an act of requesting proof of the values of one or more measurable aspects of the requesting computer system*(signed message contains random challenge and Diffie-Hellman key exchange value)* [column 8, lines 33-39].

Claims 21 and 32: Traw et al. discloses a method and computer program product for authorizing the requester to interact with the provider, the method comprising:

a. an act of sending a request to the provider*(devices exchange challenges)* [column 7, lines 6-15];

b. an act of receiving a configuration challenge from the provider, the configuration challenge indicating how the requester is to prove that the requester is appropriately configured to interact with the provider*(devices exchange challenges)* [column 7, lines 6-15];

c. an act of sending proof*(response)* of the values of one or more measurable aspects of the requester to the provider [column 7, lines 6-15];

d. and an act of receiving a token*(control channel key)* that can be used to prove that the requester is appropriately configured [column 7, lines 42-55].

Claim 22: Traw et al. discloses a method as in claim 21 above and further discloses that the act of sending a request to the provider comprises an act of sending a challenge along with the request, the challenge indicating how the provider is to prove that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 23: Traw et al. discloses a method as in claim 21 above and further discloses that the act of receiving a configuration challenge from the provider comprises an act receiving a configuration challenge along with proof*(response)* that the provider is appropriately configured to issue configuration challenges to the requester [column 7, lines 6-15].

Claim 24: Traw et al. discloses a method as in claim 21 above and further discloses that the act of sending proof*(response)* of the values of one or more measurable aspects of the requester to

the provider comprises an act of sending a challenge along with the proof*(response)* of the values of one or more measurable aspects, the challenge indicating how the provider is to prove that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 25: Traw et al. discloses a method as in claim 21 above and further discloses an act of receiving a token comprises an act of receiving a token*(control channel key)* along with proof*(response)* that the provider is appropriately configured to issue configuration challenges to the requester [column 7, lines 6-15 & lines 42-55].

Claims 26 and 33: Traw et al. discloses a method and computer program product for authorizing the requester and the provider to interact with the provider, the method comprising:

a. an act of receiving a request from the requester*(devices exchange challenges)* [column 7, lines 6-15];

b. an act of causing a configuration challenge to be issued to the requester, the configuration challenge requesting proof that the requester is appropriately configured to interact with the provider*(devices exchange challenges)* [column 7, lines 6-15];

c. an act of receiving proof*(response)* of the values of one or more measurable aspects of the requester's configuration [column 7, lines 6-15];

d. and an act of sending a token*(control channel key)* that can subsequently be used to prove that the requester is appropriately configured [column 7, lines 42-55].

Claim 27: Traw et al. discloses a method as in claim 26 above and further discloses that the act of receiving a request comprises an act of receiving a challenge along with the request, the

challenge requesting proof that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 28: Traw et al. discloses a method as in claim 26 above and further discloses that the act of causing a configuration challenge to be issued to the requester comprises an act of sending a configuration challenge along with proof*(response)* that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 29: Traw et al. discloses a method as in claim 26 above and further discloses that the act of receiving proof of the values of one or more measurable aspects of the requester's configuration comprises an act of receiving a challenge along with the proof*(response)* of the values of the one or more measurable aspects, the challenge requesting proof that the provider is appropriately configured to issue configuration challenges to the requester*(devices exchange challenges)* [column 7, lines 6-15].

Claim 30: Traw et al. discloses a method as in claim 26 above and further discloses that the act of sending a token comprises sending a token*(control channel key)* along with proof*(response)* that the provider is appropriately configured to issue configuration challenges to the requester [column 7, lines 6-15 & lines 42-55].

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2, 6, 7, 9, 12-20 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traw et al. (6,542,610).

Claims 2 and 9: Traw et al. discloses a method as in claims 1 and 8 above, but does not explicitly disclose determining that the providing computing system is appropriately configured to issue challenges to components included in the requesting computing system comprises an act of establishing an SSL connection between the requesting computing system and the providing computer system. However, it would have been obvious to one of ordinary skill in the art at the time of invention to employ an SSL connection or any other form of secure connection between two computers when transmitting sensitive data across a network. One would have been motivated to do so in order to increase the integrity of the system.

Claims 6, 7, 12 and 13: Traw et al. discloses a method as in claims 1 and 8 above and further discloses that the exchanged device certificates can provide property information about the devices being authenticated [column 8, lines 18-20], but does not explicitly disclose that the submitted assertion indicates either the identity of one or more portions of the requesting instructions or the execution environment, nor that the act of receiving proof that the requesting instructions are appropriately configured for accessing the resource comprises an act of receiving proof of the values of either the identity of one or more portions of the requesting instructions or measurable aspects of the execution environment. However, it would have been obvious to one of ordinary skill in the art at the time of invention to identify the requesting instruction or execution environment as property information about the device being authenticated and furthermore receive proof of the identity or execution environment determine if the requesting

instruction is appropriately configured. One would have been motivated to do so in order to increase the security of the authentication by employing a more comprehensive verification scheme.

Claims 14 and 31: Traw et al. discloses a method and computer program product for generating a challenge and pre-computing answers to the challenge, the method comprising:

a. an act of accessing a first random value*(random challenges)* [column 7, lines 6-15];

b. an act of accessing a secret value*(key Su)* [column 7, lines 6-15];

c. an act of using the first random value and encrypting it with the secret value to generate a second random value*(both devices respond by encrypting and then hashing the other device's challenge)* [column 7, lines 6-15]. The examiner notes that encrypting a random value will inherently generate another random value;

d. an act of using the first random value and the second random value as input to a second hash algorithm to pre-computer a valid answer(*both devices respond by encrypting and then hashing the other device's challenge)* which contains property information about the devices being authenticated*(the exchanged device certificates can provide property information about the devices being authenticated)* [column 7, lines 6-15 and column 8, lines 18-20]. However, Traw et al. does not explicitly disclose an act of using the first random value and the secret value as input to a first hash algorithm to generate a second random value. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to use a hash algorithm or any other encryption method when encrypting the first random value with the secret value. One would have been motivated to do so in order to facilitate the encryption step by using a known method of encrypting.

Furthermore, Traw et al. does not explicitly disclose:

a. an act of using the first random value and the second random value as input to a second hash algorithm to identify one or more regions within a portion instructions;

b. an act of retrieving values from the identified regions;

c. and an act of pre-computing an answer to the challenge based on the retrieved values. However, it would have been obvious to one of ordinary skill in the art at the time of invention to identify regions of the portion instructions as part of the property information about the device being authenticated and retrieve the values from these regions to calculate an answer to the challenge. One would have been motivated to do so in order to increase the security of the authentication by employing a more comprehensive verification scheme.

Claim 15: Traw et al. discloses a method as in claim 14 above, but does not explicitly discloses that the act of accessing a first random value comprises an act of accessing a seed nonce. However, it would have been obvious to one of ordinary skill in the art at the time of invention to use a seed nonce as the first random value. One would have been motivated to do so in order to increase the integrity of the system by employing a random value that will only be used once, such as a time and date stamp value, which can never repeat.

Claim 16: Traw et al. discloses a method as in claim 14 above, but does not explicitly disclose that the act of using the first random value and the secret value as input to a first hash algorithm to generate a second random value comprises using a seed nonce and the secret value to generate a challenge nonce. However, it would have been obvious to one of ordinary skill in the art at the time of invention to use a seed nonce as the first random value. One would have been motivated

to do so in order to increase the integrity of the system by employing a random value that will only be used once, such as a time and date stamp value, which can never repeat.

Claim 17: Traw et al. discloses a method as in claim 14 above, but does not explicitly disclose that the act of using the first random value and the second random value as input to a second hash algorithm to identify one or more regions within a portion instructions comprises an act of using a seed nonce and a challenge nonce as input to the second hash algorithm to generate a random bit stream. However, it would have been obvious to one of ordinary skill in the art at the time of invention to use a seed nonce as the first random value. One would have been motivated to do so in order to increase the integrity of the system by employing a random value that will only be used once, such as a time and date stamp value, which can never repeat. The examiner notes that encrypting a nonce value will inherently result in another nonce value(challenge nonce) and that hashing random values will inherently result in a random bit stream.

Claim 18: Traw et al. discloses a method as in claim 14 above and further discloses that the portion of instructions comprises a plurality of identified regions*(generates a random challenge and concatenates it with a digital certificate to form a data string)* [column 7, lines 16-20].

Claim 19: Traw et al. discloses a method as in claim 14 above and further discloses that the computing system includes a challenge service, further comprising:

a. an act of receiving a request for a challenge that a provider can subsequently issue to a requester*(devices exchange challenges)* [column 7, lines 6-15];

b. and an act of returning the identified one or more regions within a portion instructions and the values retrieved from the identified regions to the provider*(response)* [column 7, lines 6-15].

Claim 20: Traw et al. discloses a method as in claim 14 above and further discloses that the computing system includes a challenge service, further comprising:

a. an act of receiving a response that was submitted to a provider as a response to a challenge generated by the challenge service, reception of the response indicating that the response was not a pre-computed answer to the challenge*(if it does not match its expected value, then Device A and Device B cannot exchange protected content)* [column 7, lines 39-41];

b. an act of verifying the response*(each device verifies that the appropriate response has been received)* [column 7, lines 6-15];

c. and an act of indicating to the provider that the response is valid*(if the random challenge is successful, a shared control channel key is computed by the devices)* [column 7, lines 6-15].

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Diffie et al. (5,371,794).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 6:30AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James W. Myhre can be reached on (571) 270-1065. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
April 25, 2007

***

James W. Myhre
Supervisory Patent Examiner

KIEU VU
PRIMARY EXAMINER